SYNOPSIS

ON

THREATS DETECTION TO TROUBLESHOOT CYBER SECURITY CHALLENGES IN THE AUTOMOTIVE ECOSYSTEM USING ARTIFICIAL INTELLIGENCE

Research Supervisor:

Dr. Gireesh Kumar Dixit

Associate Professor

Research Scholar:

T. Ruth Supriya

Reg.No.8018722010003

Department of Computer Science & Information Technology

Shyam Univesrity, Dausa (Rajasthan), India

Year: 2024

I. INTRODUCTION

1.1 BACKGROUND OF THE STUDY

Artificial intelligence (AI) is an area of study that has the potential to drastically alter society's usage of information technology, especially in terms of how personal data will be linked and how hackers will get access to private lives. Profit-driven criminals are expected to tailor future AI software systems to their activities, confounding current cybercrime investigations further. This thesis looks at how transnational criminal organizations and cybercriminals may use emerging AI technology to carry out increasingly complex criminal operations, as well as what measures the homeland security industry should take to prepare. Four scenarios were created using a future scenario approach to predict how hackers could exploit AI systems and what can be done now to safeguard the US from harmful AI usage.

Many areas of automotive technology have progressed. Autonomous cars are closer to commercialization as a result of these advances, which have spawned a complex automotive technology ecosystem. These advancements, like any other technology, provide advantages while also posing a number of dangers. Cybersecurity hazards are one of these concerns in the automobile industry. In the case of automobiles, these security issues may have catastrophic consequences and high expenses, including the loss of life. As a result, performing a thorough threat analysis, assessment, and detection eliminates some of the automotive ecosystem's cybersecurity issues. This dissertation will do this by constructing a three-step framework that uses machine learning algorithms to evaluate, appraise, and identify risks.

1.2 ARTIFICIAL INTELLIGENCE

Since the 1990s, technological advancements have resulted in a substantial improvement in the way individuals execute various jobs. The capacity to learn and use various skills and information to solve an issue is referred to as intelligence. Intelligence also include the use of broad mental abilities to solve, reason, and learn different circumstances. Language, attention, planning, memory, and perception are all cognitive skills that are linked to intelligence. In general, the development of intellect may be examined in the past 10 years. Human and Artificial Intelligence are both involved in intelligence. The idea of AI as a science was closer to science fiction. However, AI is no longer a science fiction, but rather a

fact that has become a part of our everyday life. As a result, AI enables computers to analyze complicated data and deliver correct information via the use of neural networks that replicate the actual operations of real neurons.

Artificial Intelligence (AI) is a branch of science and engineering concerned with the theory and practice of creating systems that show the qualities of intelligence in human behavior. AI has become a major study topic in many areas in the twenty-first century, including engineering, science, education, health, business, accounting, finance, marketing, economics, stock market, and law, to name a few. The golden era of AI has arrived, thanks to AI breakthroughs and progress. As a consequence, artificial intelligence has become the most sophisticated technology. As a result, it will continue to dominate the technological spotlight for many years. It is essential to highlight that artificial intelligence has enhanced people's lives. Integration of AI technology, in particular, has a strong link to enhancing people's activities in their daily lives.

Since the intelligence of computers with machine learning skills has had significant effects on industry, governments, and society, the scope of AI has expanded dramatically. The fields of artificial intelligence are divided into 16 groups on a wide scale. Reasoning, programming, artificial life, belief revision, data mining, distributed AI, expert systems, genetic algorithms, systems, knowledge representation, machine learning, natural language understanding, neural networks, theorem proving, constraint satisfaction, and theory of computation are some of the topics covered.

While some developed systems, such as an expert or a planning system, can be classified as pure AI applications, the majority of AI systems are developed as components of complex

applications to which they add intelligence in a variety of ways, such as allowing them to reason with knowledge, process natural language, or learn and adapt. Artificial Intelligence is a vast multidisciplinary subject having origins in and connections to a wide range of disciplines, including mathematics, linguistics, psychology, neurology, mechanical engineering, statistics, economics, control theory and cybernetics, philosophy, and many more. Many ideas and techniques from these areas have been taken, but it has also contributed.

1.3 CYBERSECURITY

In many respects, the internet has made the globe smaller, but it has also exposed us to never-before-seen influences that are both diverse and difficult. "The hacking world expanded at the same rate as security." There are two approaches to the problem of cyber security. One is that cloud computing firms only do that, therefore these businesses will be very well protected using the most cutting-edge encryption technology. Because more than 60% of all commercial transactions are now conducted online, this sector necessitated a high level of security to ensure transparent and efficient transactions. As a result, cyber security has become a hot topic. The scope of cyber security extends beyond protecting information in the IT sector to include a variety of other areas such as cyber space. Cloud computing, mobile computing, E-commerce, online banking, and other cutting-edge technologies all require a high degree of security. Because these technologies contain sensitive information about a person, their security has become a priority.

The digitalization of many areas of human life, such as healthcare, education, and business, has progressively led to the storing of a wide range of data, including sensitive information. Security is the act of safeguarding digital information against theft or physical harm while preserving the information's confidentiality and availability. However, as technology advances, the quantity and complexity of cybercrime grows. The use of insufficient software, expired security measures, design faults, programming mistakes, readily accessible internet hacking tools, lack of public knowledge, high rates of financial returns, and other factors are all contributing to this massive increase in cybercrime. Technical attackers create increasingly sophisticated attack tools in order to investigate the target's weaknesses and therefore attack the victim. This has resulted in the emergence of new assaults in a variety of forms that are difficult to detect. The development of efficient security algorithms has been aided by an increase in internet dependence in all areas of life, the digital character of data in

large quantities accumulating via online transactions, and the decentralization of data repositories. Because of the ever-changing nature of cybercrime, it's tough to keep up with and prevent new risks. Because sophisticated threats play such a large role in cyberspace, it is the most demanding and hard job. As a result, it is essential to get knowledge of security defensive mechanisms, various methods, and current issues in the field of information security.

Cyber security is a collection of methods described in published documents that aims to protect a user's or organization's cyber environment. It is in charge of the methods that are used to protect networks, applications, and data from unwanted access. It may also be referred to as information technology security since it encompasses a wide range of technologies and procedures. The area is becoming more important as people become more reliant on computer systems, such as smartphones, TVs, and the many little gadgets that make up the Internet of Things.

Today, cybersecurity plays a critical role in ensuring our society's security. Cybersecurity, on the other hand, is neither a simple word nor a well-defined sub-domain of a single academic field. It has evolved into a highly cross-border and constantly changing field throughout time, making it impossible to comprehend its entire scope at a single look. Enhancing cyber security and safeguarding key information infrastructures are crucial to the security and economic well-being of any country. Making the Internet safer (and safeguarding Internet users) has become a key component of both new service development and government regulation. The battle against cybercrime requires a more comprehensive and secure strategy. Given that technological measures alone cannot prevent any crime, it is essential that law

enforcement authorities be given the tools they need to successfully investigate and prosecute cybercrime. Many countries and governments are now enacting stringent cyber security legislation in order to avoid the loss of sensitive data. Every person must be educated in cyber security in order to protect oneself from the growing number of cyber-crimes.

1.4 AI FOR CYBERSECURITY

Cybersecurity may utilize AI to enhance awareness, respond in real-time, and improve overall efficacy, just as AI-systems need new cybersecurity tools and techniques to improve their trustworthiness and resilience. This involves self-adaptation and adaptability in the face of continuous assaults that change the existing attacker-defender imbalances. Strategies that utilize AI to classify different types of assaults and educate adaptive responses (e.g., discover inconsistencies fast and know how to fix them) at scale may use AI to identify an adversary's vulnerabilities, apply observation methods, and collect lessons learnt. It is well known that a small group of skilled cyber defenders can successfully secure networks that are utilized by tens of thousands of people. AI may extend that same degree of system security, making it ubiquitous, as well as providing the domain knowledge needed to handle issues like quality-of-service limitations and system degradation behaviors.

In cyber defensive situations, AI is likely to be utilized by both attackers and defenders, unlike other successful AI applications (e.g., spam filtering). With the inclusion of AI, the conventional approach of removing vulnerabilities or raising the cost of an attack changes. Both autonomous and semiautonomous (human-in-the-loop) systems will need to prepare for worst-case scenarios as well as predict, react to, and evaluate possible and actual threat occurrences. AI-based choices impact a wide range of stakeholders, including data owners, service providers, and system administrators. Important issues include how stakeholders are engaged and informed about autonomous operations, as well as how decision-making is delegated and restricted. In a stable cyber environment, attacks could use classic deterministic planning; in an uncertain cyber environment, attacks could involve planning under uncertainty; and when little is known about the environment, the attacker could use AI to gather information, learn how to attack, conduct reconnaissance, and develop strategies.

Artificial intelligence (AI) can collect and analyze the massive amounts of data generated by today's technological systems. As a result, this capability offers the necessary training data for AI system invention and development. AI-based reasoning that is aligned with

cybersecurity objectives may improve the trustworthiness of both completely automated and human-in-the-loop systems. The development and implementation of more dependable software systems, as well as identity management, are two possible topics. AI is being used to detect mistakes in programs, verify best practices, discover security vulnerabilities, and make it simpler for software developers to incorporate security into their systems, according to promising study.

Identity management and access control are another potential use of AI. By stealing permission tokens, adversaries may undermine a variety of methods. A lightweight, transparent, and difficult-to-evade approach based on a history of contacts and anticipated behavior may be used by an AI-based system. AI may improve accuracy and decrease risks in biometric authentication systems. The tracking of behavioral patterns by AI, on the other hand, may result in privacy breaches. More study is required to create approaches that address both the ethical and technological elements of AI-assisted identity management, as well as the potential for misuse.

II. REVIEW OF LITERATURE

Zhimin et al (2021) Artificial intelligence (AI) methods have been attempted in a wide variety of cyber security applications in recent years. As a result, this article reviews the current literature on AI applications in user access authentication, network situation awareness, hazardous behavior monitoring, and abnormal traffic detection (which includes 54 publications mostly published between 2016 and 2020). This article also highlights certain limits and difficulties, and a conceptual human-in-the-loop intelligence cyber security model is provided based on the results.

Thanh Cong Truong, Quoc Bao Diep, and Ivan Zelinka (2020)intends to provide an overview of how artificial intelligence may be utilized in both attack and defense in the context of cybersecurity. According to the research, dramatic advancements in information technology have resulted in the creation of new cybersecurity concerns. Cyber-attacks' computational complexity necessitates new methods that are more resilient, scalable, and adaptable. The use of the AI-based method in cybersecurity problems is the subject of this essay. In particular, we show how AI may be used in malware detection, intrusion detection, APT, and other areas like spam and phishing detection. Furthermore, our paper presents a scenario in which AI might be used for malevolent purposes. Although the role of AI in addressing cybersecurity issues is still being investigated, some of the issues surrounding the deployment of AI-based defenses are also noteworthy. The adversarial assault on AI models, for example, or the development of autonomous intelligent malware. As a result, research into finding answers to these dangers should be pursued further.

Shidawa Baba Atiku et al (2020)explores the use of artificial intelligence (AI) to improve cyber security. Artificial intelligence has advanced to the point that it has surpassed human competence in jobs like data analytics. Data was gathered from Google scholar, scientific direct, research gates, academia, and other sources for this study, which used the thematic literature review approach. The study showed that using AI to control cyber-attacks has both benefits and drawbacks; nevertheless, the benefits exceed the drawbacks. This study finds that AI systems are likely to enhance the security of consumers and companies in cyberspace due to the fast and efficient technology needed to run them. This is shown by the growing use of AI engines in cyber security rather than traditional scanning engines. The danger of adversarial AI assaults and the human factor's complacency are two of the difficulties of AI

applications for cyber security. Despite the disadvantages of the increased use of AI in cyber security, it is still thought that the benefits exceed the risks. Cyber security still requires a human aspect. As a result, more industry experts are advocating that AI should be incorporated into each company's cyber security operation center's systems.

Kirti Raj Bhatele, Harsh Shrivastava and Neha Kumari (2019) According to researchers, artificial intelligence technology will be incorporated in nearly all new software products and services by 2020, resulting in a significant shift in the way people work, live, and do business. Though AI is still in its infancy, it has already shown its limitless potential in completing tasks quickly and correctly across a wide range of sectors, including manufacturing, retail, education, healthcare, and cyber security. Without a question, if AI is properly deployed and taught, it can enhance cyber security in a variety of ways. With less resources, it can defend against cyber-attacks in real time. As cyber dangers evolve, data explodes with new patterns that are difficult to collect and evaluate for human analysts but can be crushed down in seconds by a machine learning method. Human analysts may concentrate on analyzing the findings and developing new methods for proactively combating criminals using the power of deep analysis offered by Machine learning. As a result, incorporating deep learning and machine learning into defensive systems will undoubtedly raise cyber security intelligence to new heights.

Petri Vähäkainu and Martti Lehto (2019)focuses on artificial intelligence dangers and hazards, as well as how AI might aid in the resolution of cyber security issues. The taxonomy categorization concept is used in this research to categorize 12 of the most important aspects of cyber security. The study's research approach was to collect 11 AI solutions that were classified into seven distinct categories of critical cyber security sectors, as described in the introductory chapter. Artificial intelligence is used in identifying and forecasting information security risks and abnormalities, as well as preventing them, according to the AI solutions collected. The goal of this research is to categorize AI-based cyber security solutions that have been collected and to give information on what they may provide in terms of addressing cyber security issues. Several cyber security solutions and technologies are now available to meet the requirements of businesses. The difficulty is the fragmentation of solutions and tools, as well as challenges with the installation and maintenance of new systems, all of which create management issues and add to the overall system's complexity. Because of the complexity of systems, they must be developed as interconnected systems that can detect

both external and internal threats and have complete cyber security built in. Within the IT architecture of the whole company, the system under development must incorporate intelligent analytic solutions. The system must be able to recognize both internal and external operations inside the business. Information security capabilities must be included into the IT architecture. Symptoms of a network assault, such as an irregular login to a server holding important data or questionable cloud service use, should be detected and responded to promptly by the system. Because an organization may encounter up to 200 000 information security events each day, new methods to identify risks are required. Investigating incidents with the help of human information security experts is both costly and time-consuming.

Zarina I., Khisamova, Ildar R., Begishev and Elina L., Sidorenko (2019) The research identified the most common kinds of criminological hazards linked to AI deployment. The authors looked at the problems of assigning blame and compensating for harm produced by AI in a different question. The authors argue for the need of recognizing AI as a source of increasing risk. It is suggested that the legal fictional be used as a way for seeing a specific legal personality of AI as a non-standard legal stance that differs from reality. Today, it is not only and not so much the law that influences the evolution of relationships in the field of using digital technologies, as the latter compel people to transform and interact with other regulators in order to use digital technologies for their own self-development at various levels of life. Artificial intelligence is one of these technologies. In terms of endowing an autonomous AI with the duty to bear responsibility for damage and bad consequences, we believe the best approach is to endow AI with a particular limited legal personality (via the use of legal fiction). This approach will very certainly need a reconsideration of fundamental criminal law postulates and concepts, particularly the institutions of the subject and the subjective aspect of crime. Simultaneously, we believe that AI systems will need the establishment of a separate criminal justice institution, distinct in its core and substance from the conventional anthropocentric approach. A totally different strategy is required for such a legal organization. Within the framework of this institution, it seems appropriate to provide for a different understanding of the subject, based on the symbiosis of technical and other characteristics of AI, as well as alternative types of responsibility, such as deactivation, reprogramming, or endowing with the status of criminal, which will serve as a warning for all legal relators. We think that in the future, such a solution will be able to reduce the criminological dangers associated with AI.

Kaspersky Lab (2018)states that cyber security is a technique for preventing unauthorized harmful assaults on computers, servers, mobile devices, electronic systems, networks, and data. Cyber security is a wide term that encompasses anything from personal computer information security to disaster recovery and end-user training. Artificial intelligence and cyber security are inextricably linked. Cyber security, according to Lord (2017), refers to technology, procedures, and practices that are intended to safeguard networks, devices, programs, and data against attack, damage, or illegal access. Information technology security is another term for cyber security.

Buczkowski, (2017) Artificial intelligence is a broad phrase that may be used to describe a variety of technologies. Its goal is to let computers to think as humans do, to imitate human behaviors, and to solve problems quicker and more effectively than people can. AI may be used to do a variety of activities, including creative, planning, movement, speaking, object and sound identification, as well as social and commercial interactions. Evidence-based techniques, natural language processing (NLP), text mining, predictive and prescriptive analytics, recommendation systems, machine and deep learning may all be used to complete tasks. The methods described above may also be utilized to address cyber security issues..

Lehto, (2015) Cyber security procedures are linked to risk management, vulnerability patching, and system resilience. Techniques for identifying various network behavior abnormalities and viruses, as well as IT issues linked to IT security, are among the main study topics. In a nutshell, cyber security is a set of activities done to protect against cyber-attacks and their effects, which includes putting in place the necessary countermeasures. An organization's or institution's threat analysis is the foundation for cyber security. The structure and components of a company's cyber security strategy, as well as its execution program, are based on threat and risk assessments. In many instances, a business may need to develop multiple focused cyber security plans and standards. The essential element is that required dangers will be prepared for, and enough protection against threats' harmful consequences will be tried to be established. Enhancing the fundamentals of cyber security, raising everyone's awareness of risks, improving operational capacity, and preserving security are the best ways to prepare for cyber threats. The main problem is recognizing cyber security threats and being able to react properly. Being able to operate in the face of a cyber-attack, as well as quickly ending the assault and restoring the organization's operations to their former regular

condition before to the event, is an essential aspect of cyber security. To address these problems, appropriate laws and a more in-depth discussion are required.

III. PROBLEM STATEMENT

Although cybersecurity in automotive systems is a well-studied topic, intrusion detection methods in V2X BSM datasets have yet to be investigated. There aren't many comprehensive studies on V2X cybersecurity in terms of threat analysis, assessment, and detection since linked automobile technology hasn't been extensively implemented and marketed. There are a variety of threat assessment and characterization models available, including EVITA, NHTSA, HEAVENS, OCTAVE, and others. These threat assessment methods are critical for private companies trying to identify the severity of a threat, but there is no established framework that utilizes and incorporates the result in the design of other security systems (i.e., intrusion detection systems). The goal of this research is to find a link between threat assessment and intrusion detection methods. All of the danger or risk evaluations in this research will be done subjectively, utilizing tables or scoring. The threat categorization assignment will not be done using discrete variables throughout this procedure. They will often be evaluated using linguistic factors and non-discrete definitions from the perspective of the users. This threat assessment method often results in inefficient scoring and incorrect judgments because to the Fuzzy nature of the procedure. This study is one of the first to try to address threat assessment inefficiencies using a Fuzzy logic approach. Because there aren't enough publicly accessible V2X or DSRC datasets for study, there aren't many findings. This research will make advantage of one of the most recent datasets in the area. When it comes to intrusion detection systems in the automotive V2X space, they are often dismissed as a viable option owing to a large number of false positives or expensive computing needs. The goal of this study is to come up with a workable IDS for implementation.

IV. OBJECTIVES OF THE STUDY

The main Objectives of the Research study are stated as follows:

1. To study the concept of Artificial Intelligence and Cybersecurity
2. To develop a Two-stage Intrusion Detection System using supervised and unsupervised learning
3. To analyze the Use of the Fuzzy Logic methodology to increase the efficiency and accuracy in threat assessment models
4. To analyze the Threats Detection to troubleshoot cybersecurity challenges in the automotive ecosystem Using Artificial Intelligence

V. RESEARCH METHODOLOGY

5.1 RESEARCH STRUCTURE

These steps are provided below and follow their respective methodologies.

Step 1: An analysis of automotive threats with a focus on V2X will be done. This dissertation attempts to stay close to established standards, so the proposed solution will have a higher chance of implementation and adoption. In this step, Microsoft STRIDE model will be used for threat analysis.

Step 2: The evaluation step will result in the creation of a Fuzzy-based Threat Assessment Model (FTAM). Five existing models will be used to benchmark and guide the design of the new proposal at this stage. FTAM aims to fill up the gaps found in the literature study for models, as well as remove or minimize their disadvantages. Despite the fact that a new model will be presented, all danger classification levels will be based on existing models. A multistage approach will be utilized from the viewpoint of fuzzy logic. Building six Fuzzy inference systems takes time, but all of the Fuzzy rules are taken into consideration since anything might happen.

Step 3: The goal of the third detection step is to create an intrusion detection system. This stage's technique is comparable to a two-stage architectural approach described in earlier publications. This technique will be tested to see whether it can decrease false positives, reduce data bias, and reduce computing needs in a range of applications (vision and cybersecurity). The first step seeks to merely identify a danger, while the second tries to categorize it in order to improve accuracy and reduce false positives.

VI. EXPECTED OUTCOME

Artificial intelligence (AI) is an area of study that has the potential to drastically alter society's usage of information technology, especially in terms of how personal data will be linked and how hackers will get access to private lives. Profit-driven criminals are expected to tailor future AI software systems to their activities, confounding current cybercrime investigations further. At the application, network, host, and data layers, cybersecurity solutions are needed. "The goal of the study is to see how well Artificial Intelligence paradigms function in network detection and prevention systems." This project aims to create a cyber-security system that employs artificial intelligence principles and can deal with a high level of complexity. Using Artificial Intelligence, this thesis will investigate Threats Detection to troubleshoot cybersecurity issues in the automobile industry.

REFERENCES

[1]. Buczkowski, A. 2017. What's the Difference Between Artificial Intelligence, Machine Learning and Deep Learning? GEO. Retrieved by http://geoawesomeness.com/whats-difference-artificial-intelligence-machine-learning-deep-learning

[2]. Kasperskylab. 2018. What is Cyber-Security?AO Kaspersky Lab. Retrieved by https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security

[3]. Kirti Raj Bhatele, Harsh Shrivastava and Neha Kumari (2019) The Role of Artificial Intelligence in Cyber Security Countering Cyber Attacks and Preserving the Integrity and Availability of Critical Systems (pp.170-192). DOI:10.4018/978-1-5225-8241-0.ch009

[4]. Lehto,M. 2015. Phenomena in the Cyber World.M. Lehto & P. Neittaanmäki (Edit.) Cyber Security: Analytics, Technology and Automation. Berlin: Springer.

[5]. Lord, N. 2017. What is Cyber Security? Data Insider. Retrieved by https://digitalguardian.com/blog/what-cyber-security

[6]. Petri Vähäkainu and Martti Lehto (2019) Artificial intelligence in the cyber security environment The 14th International Conference on Cyber Warfare and Security ICCWS2019. https://www.researchgate.net/publication/338223306_Artificial_intelligence_in_the_cyber_security_environment_Artificial_intelligence_in_the_cyber_security_environment

[7]. Shidawa Baba Atiku, Achi Unimke Aaron, GotengKuwunidi Job, Fatima Shittu and Ismail Zahraddeen Yakubu (2020) Survey on The Applications of Artificial Intelligence in Cyber Security International Journal of Scientific & Technology Research Volume 9, Issue 10, ISSN 2277-8616

[8]. Thanh Cong Truong, Quoc Bao Diep, and Ivan Zelinka (2020) Artificial Intelligence in the Cyber Domain: Offense and Defense Symmetry 2020, 12, 410; doi:10.3390/sym12030410 www.mdpi.com/journal/symmetry

[9]. Zarina I., Khisamova, Ildar R., Begishev and Elina L., Sidorenko (2019) Artificial Intelligence and Problems of Ensuring Cyber Security 2019 International Journal of Cyber Criminology – ISSN: 0974–2891 July – December 2019. Vol. 13(2): 564–577. DOI: 10.5281/zenodo.3709267

[10]. Zhimin Zhang, Huansheng Ning, Feifei Shi, Fadi Farha, Yang Xu, Jiabo Xu, Fan Zhang & Kim-Kwang Raymond Choo (2021) Artificial intelligence in cyber security: research advances, challenges, and opportunities *ArtifIntell Rev* (2021). https://doi.org/10.1007/s10462-021-09976-0